VIII kadencja

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Infrastruktury**
(nr 265)
z dnia 20 lutego 2019 r.

Pełny zapis przebiegu posiedzenia

Komisji Infrastruktury (nr 265)

20 lutego 2019 r.

Komisja Infrastruktury, obradująca pod przewodnictwem posła **Bogdana Rzońcy (PiS)**, przewodniczącego Komisji, rozpatrzyła:

– informację na temat zagrożeń w cyberprzestrzeni związanych z funkcjonowaniem transportu kolejowego oraz działań podjętych w tym zakresie w kontekście tworzenia Narodowej Platformy Cyberbezpieczeństwa.

W posiedzeniu udział wzięli: **Adam Andruszkiewicz** sekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Tomasz Buczyński** dyrektor Departamentu Kolejnictwa Ministerstwa Infrastruktury wraz ze współpracownikami, **Ignacy Góra** prezes Urzędu Transportu Kolejowego, **Jakub Prusik** p.o. prezesa PKP Informatyka wraz ze współpracownikami, **Tomasz Emiljan** dyrektor Departamentu Infrastruktury Najwyższej Izby Kontroli wraz ze współpracownikami, **Sławomir Szumilas** zastępca dyrektora Biura do Walki z Cyberprzestępczością w Komendzie Głównej Policji wraz ze współpracownikami, **Robert Sobczak** członek zarządu PKP PLK wraz ze współpracownikami.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Elżbieta Kessel**, **Jakub Sindrewicz** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Bogdan Rzońca (PiS):

Otwieram posiedzenie Komisji Infrastruktury. Drodzy państwo, porządek dzienny obejmuje rozpatrzenie informacji na temat zagrożeń w cyberprzestrzeni związanych z funkcjonowaniem transportu kolejowego oraz działań podjętych w tym zakresie w kontekście tworzenia Narodowej Platformy Cyberbezpieczeństwa. Informację przedstawia minister cyfryzacji oraz prezes PKP Informatyka. Panu ministrowi wraz z zespołem i panu prezesowi wraz z zespołem bardzo dziękujemy za obecność. Witam zaproszonych gości, witam sekretarza stanu pana Adama Andruszkiewicza wraz z zespołem. Mamy także reprezentantów Ministerstwa Infrastruktury – pan dyrektor Departamentu Kolejnictwa Tomasz Buczyński, wicedyrektorzy Tomasz Rurka i Jakub Kapturzak oraz Magdalena Kossowska, Maciej Sofiński i Karol Przeździecki. Ministerstwo Spraw Wewnętrznych i Administracji reprezentuje pan Sławomir Szumilas, zastępca dyrektora Biura do Walki z Cyberprzestępczością w Komendzie Głównej Policji. Jest też pani Karolina Dubis, Michał Zugaj, Marcin Kuskowski. Jeśli będzie potrzeba, państwo się później przedstawią. Schodzimy już na poziom spółek – PKP Informatyka, a mianowicie jest z nami pan prezes Jakub Prusik oraz członkowie zarządu: Radosław Zawierucha, Robert Milewski i Artur Ślubowski oraz Filip Chrzanowski, rzecznik prasowy. PKP PLK reprezentuje pan Robert Sobczak, członek zarządu do spraw rozwoju, oraz pan Mirosław Majsterek, członek zarządu, dyrektor Biura Informatyki, i Jan Danowski, naczelnik wydziału w Biurze Informatyki. Urząd Transportu Kolejowego reprezentuje pan prezes Ignacy Góra – witam serdecznie. Najwyższa Izba Kontroli – pan dyrektor Tomasz Emiljan, dyrektor Departamentu Infrastruktury, wraz z panem Maciejem Mierzejewskim.

Witam państwa posłów. Drodzy państwo, przejdziemy do zreferowania porządku dziennego. W tym wypadku uprzejmie proszę pana ministra lub wyznaczoną osobę o zabranie głosu.

Sekretarz stanu w Ministerstwie Cyfryzacji Adam Andruszkiewicz:

Szanowny panie przewodniczący, szanowni państwo posłowie, Wysoka Komisjo, szanowni goście, w Ministerstwie Cyfryzacji kompleksowo realizujemy projekt strategiczny, który wynika ze zobowiązania zawartego w „Strategii na rzecz odpowiedzialnego roz-

woju" o nazwie „Zintegrowany system zarządzania bieżącego bezpieczeństwem cyberprzestrzeni RP". System ten znalazł umocowanie prawne w art. 46 ustawy z dnia 5 lipca 2014 r. o krajowym systemie cyberbezpieczeństwa. Efektem realizacji projektu strategicznego będzie system teleinformatyczny, który zapewni: wymianę informacji na potrzeby współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa, zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym, ostrzeganie o zagrożeniach dla cyberbezpieczeństwa.

Realizacja projektu została rozłożona na projekty szczegółowe. Obecnie najistotniejsze znaczenie ma realizacja projektu o nazwie Narodowa Platforma Cyberbezpieczeństwa (NPC). Jest to projekt o charakterze badawczo-wdrożeniowym posiadający dofinansowanie z Narodowego Centrum Badań i Rozwoju. Projekt realizowany jest przez konsorcjum, którego liderem jest NASK – Państwowy Instytut Badawczy. Oprócz instytutu w skład konsorcjum wchodzą: Politechnika Warszawska, Narodowe Centrum Badań Jądrowych oraz Instytut Łączności – Państwowy Instytut Badawczy. Celem projektu NPC jest opracowanie kompleksowego, zintegrowanego systemu monitorowania, opracowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa. Wynikiem prac będzie prototyp, w skład którego wejdą centrum operacyjne i komponenty integrujące z innymi uczestnikami systemu.

Sprawdzony w warunkach operacyjnych prototyp NPC zapewni koordynację w skali kraju działań służących zapobieganiu, wykrywaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa oraz stworzy warunki do współdzielenia wiedzy o zagrożeniach między państwami UE. Rozwiązania systemowe i techniczne opracowane w ramach NPC umożliwią uzyskiwanie bieżącej informacji o stanie bezpieczeństwa w cyberprzestrzeni, ocenę zagrożeń i ich potencjalnych skutków oraz skoordynowane reagowanie na incydenty komputerowe na poziomie krajowym. Wartość dofinansowania ze strony NCBiR wynosi 20 mln 832 tys. zł. Prototyp systemu powinien być gotowy w połowie 2020 r.

Warunkiem funkcjonowania NPC jest zasilanie informacyjne przez klientów tego systemu, a w szczególności przez operatorów usług kluczowych. W związku z tym projekt nawiązał kontakt z kilkoma podmiotami, w tym z PKP Informatyka, w celu przeprowadzenia walidacji przyjętych rozwiązań. Współpraca NPC z PKP Informatyka pozwoliła na pozyskanie wielu cennych i użytecznych danych niezbędnych do oceny przyjęcia w projekcie koncepcji funkcjonowania systemu.

Równolegle Ministerstwo Cyfryzacji wraz z NASK prowadzi projekt towarzyszący projektowi NPC pod nazwą NPCnet. Celem tego projektu jest zaprojektowanie i zbudowanie sieci informatycznej łączącej centrum systemu z jego klientami. W latach 2017–2018 Ministerstwo Cyfryzacji udzieliło NASK na ten cel dotacji celowych w wysokości 896 tys. zł. Na ten sam cel w roku 2019 planowane jest udzielenie instytutowi dotacji w wysokości 1 mln 668 tys. zł. Jednocześnie w Ministerstwie Cyfryzacji trwają prace nad powierzeniem NASK zadania, którego celem byłoby zbudowanie i utrzymanie systemu docelowego, o którym mowa w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa.

Szanowny panie przewodniczący, szanowna Komisjo, jesteśmy wraz z zespołem do państwa dyspozycji. Możemy odpowiedzieć na pytania. Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję bardzo za wprowadzenie. W takim wypadku proszę o pytania, otwieram niniejszym debatę. Czy pan minister jeszcze kogoś do głosu wyznaczał? W tej chwili nie? Dobrze. Czyli PKP Informatyka. Pan prezes wraz z zespołem jest obecny, więc proszę bardzo.

P.o. prezesa PKP Informatyka Jakub Prusik:

Dzień dobry państwu. Przede wszystkim chciałbym podziękować panu przewodniczącemu i Komisji za zaproszenie. Jednocześnie, bo może nie wszyscy wiedzą, chcę podziękować za drugie zaproszenie, bo spotkaliśmy się rok temu w naszej siedzibie w Al. Jerozolimskich.

Na pograniczu tematu, czyli Narodowej Platformy Cyberbezpieczeństwa, chciałbym wspomnieć tylko, że PKP Informatyka jest nie tylko koordynatorem szeroko pojętego obszaru informatycznego, ale również budujemy, projektujemy systemy sprzedaży biletów i rezerwacji, jak również całe platformy dla przewozów pasażerskich.

Wracając do tematu Narodowej Platformy Cyberbezpieczeństwa, poprosiłbym o zabranie głosu dyrektora Biura Bezpieczeństwa Wewnętrznego, żeby omówił przygotowaną prezentację.

Przewodniczący poseł Bogdan Rzońca (PiS):

Proszę uprzejmie.

Dyrektor Biura Bezpieczeństwa i Wsparcia Użytkownika PKP Informatyka Robert Milewski:

Panie przewodniczący, panie i panowie posłowie, tutaj przedstawiamy strukturę organizacyjną Krajowego Systemu Cyberbezpieczeństwa w kontekście miejsca PKP Informatyka. Naszą ambicją i rolą, którą staramy się stworzyć, jest bycie sektorowym zespołem reagowania i podmiotem świadczącym usługi cyberbezpieczeństwa. Cała Grupa PKP bardzo ambitnie i ciężko pracuje nad stworzeniem nowego systemu cyberbezpieczeństwa. Platforma NPC wpisuje się w nasze działania. Tu jest taki ogólny schemat, gdzie widzimy PKP Informatykę. Oczywiście nie jest to przedmiotem tego posiedzenia, to jest tylko zarysowanie pewnego kształtu, gdzie my chcielibyśmy być.

Proszę o następny slajd. Z naszej perspektywy w chwili obecnej PKP Informatyka posiada Security Operations Center, które dba o bezpieczeństwo usług świadczonych dla naszych klientów. Taki SOC możemy traktować w kontekście krajowego systemu jako lokalny zespół reagowania. Naszą ambicją jest stworzenie grupowego, sektorowego zespołu reagowania, który mógłby działać w obszarze zarówno aplikacji ochrony systemu, który utrzymuje PKP Informatyka, jak również cały sektor kolejowy.

PKP Informatyka zbudowała i utrzymuje system BILKOM, który w naszym rozumieniu można traktować jako internetową platformę handlową, która dostarcza konsumentom usługi cyfrowe. Dlatego też budujemy bardzo silny zespół bezpieczeństwa, który chroni ten system. Stąd też wynika nasz udział, partycypacja w projekcie NPC, który jest przełożeniem – przynajmniej w naszym rozumieniu i zapewne w rozumieniu twórców – obowiązków wynikających z ustawy o cyberbezpieczeństwie czy dyrektywy NIS na działania bardziej praktyczne. Cały system ma za zadanie podniesienie poziomu bezpieczeństwa Rzeczypospolitej Polskiej, a sektor kolejowy jest jednym z elementów tego obszaru cyberbezpieczeństwa kraju. Dlatego też jak najbardziej przystąpiliśmy do współdziałania czy wspierania, może w skromnym zakresie, ale jednak tworzenia tej Narodowej Platformy Cyberbezpieczeństwa.

Tu chciałem przedstawić podstawowe kamienie milowe projektu NPC z perspektywy PKP Informatyka. Zaproszenie skierował do nas NASK w grudniu 2017 r. W 2018 r. prowadziliśmy rozmowy związane z warunkami przystąpienia jako uczestnika platformy NPC i formalnie w maju 2018 r. przystąpiliśmy do projektu NPC. Następnie zespoły po stronie PKP Informatyka i NASK prowadziły warsztaty analityczne i konsultacje merytoryczne z udziałem ekspertów, które miały za zadanie przede wszystkim dostarczyć dane umożliwiające podjęcie pewnych analitycznych działań po stronie NASK, ale z danych rzeczywistych z przemysłu, czyli w tym przypadku z sektora IT kolejowego.

W drugim kwartale 2019 r. jest planowane uruchomienie przez NASK demonstratora NPC i przyłączenie PKP Informatyka do systemu brzegowego wraz z jego testowaniem. Dostarczyliśmy do NASK pewne dane, które są wykorzystywane m.in. do analizy dotyczącej ryzyka.

Tak jak pan minister powiedział wcześniej, w 2020 r. planowane jest uruchomienie platformy NPC, w której chcemy uczestniczyć jako produkcyjnie aktywny podmiot.

Chciałbym tutaj przedstawić rezultaty projektu NPC. Jak pan minister wspomniał, prototypy interaktywnego systemu, ekspercki system wspomagania decyzji, metody dynamiczne i statyczne analizy ryzyka i narzędzia detekcji podatności. Ja chciałbym tylko podkreślić, że z punktu widzenia takich firm jak PKP Informatyka są to narzędzia, które wprost wspierają naszą pracę i budowanie naszego systemu bezpieczeństwa.

Tu chciałem przedstawić parę wyzwań związanych z projektem, oczywiście z perspektywy PKP Informatyka. Mamy wyzwania typu współpraca w ramach sektorowego zespołu reagowania, będzie to temat w niedługim czasie realizowany. Musimy przede wszystkim dostosować wszystkie procesy do modeli analizy statycznej czy analizy ryzyka. Dotyczy to też detekcji podatności. Naszym największym wyzwaniem jest dostosowanie procesów wewnątrz organizacji do wymagań Narodowej Platformy Cyberbezpieczeństwa, a tak naprawdę krajowego systemu cyberbezpieczeństwa. Ważne jest też pewne wyzwanie osobowe. W chwili obecnej na rynku specjalistów do spraw cyberbezpieczeństwa jest coraz mniej, każdy podmiot z rynku IT szuka tych specjalistów i próbuje ich pozyskiwać. To jest też dla nas wyzwanie, żeby zapewnić właściwe środki do utrzymania tych specjalistów i pozyskiwania środków również na zatrudnianie coraz lepszych, ale niestety też droższych specjalistów, jak również narzędzi bezpieczeństwa.

Tu chciałbym poprosić kolegę o zabranie głosu, bo chcieliśmy przedstawić nasze plany, które realizujemy, a tutaj chcielibyśmy parę słów powiedzieć o tym, co już mamy. Prosiłbym o zabranie głosu Artura Ślubowskiego, naczelnika Wydziału Bezpieczeństwa i szefa SOC PKP Informatyka.

Przewodniczący poseł Bogdan Rzońca (PiS):

Proszę bardzo.

Naczelnik Wydziału Bezpieczeństwa PKP Informatyka Artur Ślubowski:

Dzień dobry państwu. Panie przewodniczący, państwo posłowie, szanowni goście, zostałem poproszony o zaprezentowanie aspektów bardziej praktycznych, aby pokazać ten problem związany z bezpieczeństwem m.in. na kolei.

Odpowiadam w spółce za działanie SOC, czyli zespołu pracującego 24/7 nad monitoringiem dostępności funkcjonowania krytycznych procesów czy usług w państwie w obszarze kolejnictwa. W tym momencie mówię o sprzedaży biletów, rezerwacji biletów. Te systemy są przez ten zespół m.in. chronione i jest zapewnione, że są dostępne dla państwa, dla odbiorców, klientów. Część z państwa miała okazję zwiedzać nasz SOC podczas poprzedniej wizyty. Była możliwość pokazania, jak to wygląda w praktyce, jak funkcjonuje.

Gdzie jest problem? Kolej w rzeczywistości ma jeździć, przewozić, dostarczać towary, pasażerów z miejsca A do miejsca B. Informatyka dopiero wchodzi w takiej rozbudowanej formie w kolej i automatycznie wiąże się to z tym, że pojawiają się zagrożenia bezpieczeństwa z tym związane. Zagrożenia, o których chciałbym powiedzieć przykładowo, dotyczą w rzeczywistości nie tylko aspektów związanych z koleją. Te problemy dotyczą także normalnego życia, normalnej pracy biurowej w różnych spółkach. Najważniejszym od zawsze problemem jest świadomość. Możemy mieć najbardziej rozbudowane systemy informatyczne, zabezpieczenia, rozwiązania technologiczne, ale jeżeli człowiek się pomyli, jeżeli świadomie podejmie błędną decyzję, to spowoduje to największe zagrożenie. Jednym z takich zagrożeń są ataki na pracowników tzw. phishingowe, czyli są to ataki polegające na nakłonieniu odbiorcy mejla, wiadomości, żeby zaufał drugiej stronie, że jest tym kimś, za kogo się podaje. W ostatnich dniach mieliśmy przykład w Polskiej Grupie Zbrojeniowej, że ktoś otrzymał informację o zmianie numeru konta i zostały przelane duże pieniądze nie na to konto za usługę.

Są to działania wykorzystywane od wielu lat przez cyberprzestępców, polegają na nakłonieniu nas do pewnych działań. Możemy mieć zbudowany jeden, drugi, trzeci system, ale on nas przed tym nie ochroni. Może nas tylko uchronić świadomość. Jeżeli popatrzymy na pracowników firm sektora bankowego, tam liczba ataków i prób kradzieży pieniędzy jest tak duża, że oni wszyscy mają wysoki poziom świadomości. W firmach kolejowych, w których maszynista ma prowadzić pociąg, nikt nie myśli o tym, że ktoś może próbować coś zrobić. Transport wszelaki jest chyba bardziej zagrożony niż konta bankowe, największym zagrożeniem jest paraliż na wypadek, gdyby ktoś chciał sparaliżować państwo. To jest element, przed którym powinno się chronić.

Wiąże się to trochę z tym, że jeżeli mówimy o technologii kolejowej, specyficznych technologiach dedykowanych, które są stosowane w automatyce kolejowej, są to rozwiązania technologii systemów przemysłowych, które nie były przy projektowaniu – bądźmy

tego świadomi – bardzo ukierunkowane na ochronę przed atakami, nikt nie myślał, że jakiś haker może próbować się włamać i przejąć kontrolę nad systemami sterowania czy innymi związanymi z przewozami. Te systemy są najbardziej zagrożone przez taki dług technologiczny, bo istnieje ryzyko wykorzystania tych systemów w atakach i to są elementy, przed którymi należy się zabezpieczyć.

Przykład sprzed dwóch lat, czyli słynne oprogramowanie szyfrujące WannaCry, które było bardzo medialne, miało poważny efekt, ponieważ sparaliżowało kilka firm, m.in. firmę transportową Maersk, przez to, że się dostano do oprogramowania i zaszyfrowano w nim całą instalację. To dotyczyło też bankowości, można było spotkać bankomaty na świecie, Polskę bardzo mało ostatnio to dotknęło, gdzie widać było, że bankomat został zaszyfrowany. Z obszaru kolejnictwa mieliśmy Deutsche Bahn, czyli operatora w Niemczech, u którego na wyświetlaczach informacji pasażerskiej na dworcach można było zobaczyć, że zamiast skąd i dokąd można dojechać, to system prosił o opłatę w bitcoinach za odszyfrowanie danych.

Takie zagrożenia istnieją, integracja systemów informatycznych z systemami transportowymi, kolejowymi jest elementem, który jest ryzykiem, bo jest nieznany, jest nowym w rzeczywistości elementem, trwa jego budowanie. Mamy przykład w ostatnim czasie uruchamiania wi-fi w pendolino. To jest elementem łączenia kolei z internetem i nowymi technologiami. To tak informacyjnie.

Są zagrożenia, są problemy, z którymi pracownicy – my musimy sobie radzić. Musimy być świadomi tego, że one mogą dotknąć nas w najmniej spodziewanym momencie. Jednym z elementów, który w ostatnich czasach jest modnym hasłem, jest sztuczna inteligencja. Tworzy się systemy zabezpieczeń oparte na machine learningu, czyli maszynowym uczeniu się. Mechanizm, który pozwala rozpoznać w tłumie informacji zachowania generowane w rzeczywistości przez systemy hakerskie, próbujące się włamać, przełamać zabezpieczenia. Niestety, kiedy hakerzy dowiedzieli się, że takie systemy są tworzone, to dlaczego nie wykorzystać systemu sztucznej inteligencji do włamywania się, żeby on był świadomy, że po drugiej stronie jest jakaś sztuczna inteligencja, która ma go wykryć. Sztuczną inteligencję należy przełamywać sztuczną inteligencją. To jest jedna z metod. Druga metoda, każdy z nas miał już chyba możliwość zobaczyć – to jest nowy wektor ataków, o którym warto wiedzieć – chatboty na różnych stronach internetowych, gdzie można porozmawiać z automatem, który podpowie, co zrobić, w jaki sposób skontaktować się, złożyć zgłoszenie, poprosić o pomoc. Te elementy są bardzo przydatne i funkcjonalne z perspektywy użytkownika. Można kupić bilet czy usługę, wykorzystując taki automat. Tylko co będzie, kiedy ten automat zostanie złamany przez hakera i automat zamiast pomagać, będzie kierował, żeby ściągnąć plik i go zainstalować, a to w rzeczywistości będzie jakiś wirus? To są nowe wektory, które się pojawiają i które powodują, że stajemy się – przez coraz wyższy poziom integracji z systemami informatycznymi – bardziej podatni na nowe zagrożenia, nowe ryzyka.

O ryzykach można by dużo powiedzieć. To jest takie podsumowanie, skąd i dlaczego jest potrzeba takich zespołów reagowania, czyli Security Operations Center, które monitorują bezpieczeństwo, które patrzą, co się dzieje, są świadome, są wsparciem dla poszczególnych zespołów świadczących usługi, dlaczego tak ważna jest infrastruktura krytyczna, którą w jakimś sensie nasza spółka wspiera, dlaczego ochrona jest tak ważna w normalnym trybie. Stąd ta dyrektywa i stąd ustawa o krajowym systemie cyberbezpieczeństwa, stąd nasze zaangażowanie.

To tyle z mojej strony.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję bardzo. Czy jeszcze ktoś z państwa? Proszę uprzejmie.

Członek zarządu PKP Informatyka Radosław Zawierucha:

Szanowny panie przewodniczący, szanowne panie i panowie posłowie, nazywam się Radosław Zawierucha i jestem członkiem zarządu PKP Informatyka. W obszarze mojej odpowiedzialności jest m.in. Biuro Bezpieczeństwa, w tym wspomniana jednostka Security Operations Center. Tutaj są skupione odpowiedzialności za zachowanie ciągłości

operacji opiekowanych przez nas systemów i zabezpieczenia przed ewentualnymi zakusami cyberprzestępców.

Chciałbym niejako na podsumowanie powiedzieć, że krajowy system cyberbezpieczeństwa, jak my go widzimy, to jest rozwiązanie, zespół procedur, zespół rozwiązań technicznych, ludzi, który ma zapewnić cyberbezpieczeństwo Rzeczypospolitej Polskiej. My jako spółka informatyczna na rynku kolejowym widzimy możliwości i chcemy dołożyć do tej budowy cegiełkę w postaci naszego doświadczenia w tym obszarze. Jesteśmy otwarci na wszelką współpracę, która jest niezbędna, żeby ten system zbudować w sposób logiczny, sensowny, uporządkowany, a przede wszystkim skuteczny. Wymagana jest tutaj ścisła współpraca całego sektora kolejowego, wszystkich spółek. Wszystkie spółki kolejowe, czy to inwestor infrastruktury, czy przewoźnicy, czy właściciele dworców kolejowych, w takim lub innym stopniu składają się na bezpieczeństwo lub przez zaniechanie działań na brak tego bezpieczeństwa. Bezwzględnie konieczna jest więc współpraca. Do tej współpracy moja spółka jest gotowa. Istotnym elementem jest takie działanie i budowanie tego systemu oraz później jego prowadzenie, żeby działał on według określonych standardów i reguł, aby w każdym przypadku operacyjnego zagrożenia czy innego działania wymagającego reakcji nie zastanawiać się, co trzeba zrobić, tylko żeby działo się to zgodnie z procedurami, niejako z automatu.

Działania wymagają stałej troski i monitorowania w trybie 24/7/365 – to jest oczywiste. Takie działania moja spółka prowadzi już teraz. Do zbudowania krajowego systemu cyberbezpieczeństwa czy Narodowej Platformy Cyberbezpieczeństwa, która jest już konkretną emanacją tego działania, niezbędne są nakłady. To chyba jest oczywiste, że wymaga to sporych inwestycji w ludzi i w sprzęt, w oprogramowanie. Trzeba mieć tego świadomość i być na to gotowym. Ale, jak już o tym wspomniałem, kto się odpowiednio nie ubezpieczy, ten potem może stać się ofiarą i mocno tego żałować. Nic nowego tutaj nie mówię.

Na koniec chcę stwierdzić, że chciałabym, aby wiedza i kompetencje, jakie mamy zebrane w tym obszarze w naszej spółce, służyły do budowy rozwiązań Narodowej Platformy Cyfrowej, i zapewniam, że nasi ludzie i nasze jednostki są w pełni dyspozycyjne, otwarte i chętnie dołożą cegiełkę do tej budowli. Mam nadzieję, że tak się stanie. Dziękuję uprzejmie.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję. Rozumiem, że teraz możemy przejść do pytań i dyskusji. Niniejszym otwieram debatę nad przedłożoną informacją. Jeśli państwo posłowie mają w pierwszej kolejności jakieś pytania – tematyka jest frapująca, ciekawa, trudna, nawet niepowszednia, ale ogromnie ważna. Wszyscy jesteśmy narażeni na jakąś niespodziankę, funkcjonując z iPadem, telefonem, jadąc pociągiem czy korzystając z jakiejkolwiek formy elektroniki. Można powiedzieć, że wolność już była, teraz z każdej strony, nawet w tej sali wszystko, co się dzieje, jest dobrze monitorowane, nie jest to tajemnica.

Drodzy państwo, proszę o pytania, jeśli są. Jeszcze nigdy wcześniej tak nie było. Panie ministrze, panowie tak wbili w krzesła posłów… Widzę, że pan prezes idzie nam w sukurs. Proszę bardzo.

Prezes Urzędu Transportu Kolejowego Ignacy Góra:

Szanowny panie przewodniczący, Wysoka Komisjo, szanowni państwo, z punktu widzenia bezpieczeństwa prowadzenia ruchu kolejowego obszarem najbardziej newralgicznym są oczywiście urządzenia zabezpieczenia ruchu kolejowego. Biorąc pod uwagę strategię wdrażania przez państwo polskie w systemie kolejowym Europejskiego Systemu Zarządzania Ruchem Kolejowym, gdzie zarówno infrastruktura, jak i tabor kolejowy w te urządzenia będzie wyposażany, to rzeczywiście urządzenia zabezpieczenia ruchu kolejowego są z jednej strony najbardziej podatne na ataki związane z cyberbezpieczeństwem, a z drugiej strony są najbardziej wrażliwe, najbardziej zagrożone, a skutki z tego wynikające mogą być bardzo katastrofalne.

Nie ukrywam, że w wypowiedziach panów nikt do tego zagrożenia się nie ustosunkował. To jest pierwsze moje pytanie. A drugie jest takie, że PKP Informatyka, jak państwo sami wskazują w swojej prezentacji, reprezentuje interes Grupy PKP. Czy państwo zasta-

nawiali się nad tym, jak swoimi działaniami objąć pozostałe podmioty, które funkcjonują w przestrzeni kolejowej? Grupa PKP to rzeczywiście największy zarządca infrastruktury kolejowej PKP PLK, ale tych zarządców mamy jeszcze co najmniej kilku, a jeżeli chodzi o przewoźników, to jest tylko kilku przewoźników w Grupie PKP, natomiast wszystkich przewoźników w skali całego kraju jest ponad stu. Czy zastanawiamy się nad tym, jak zintegrować środowisko i rzeczywiście pomagać wszystkim podmiotom, które funkcjonują na rynku kolejowym i są zagrożone?

To obszar, o którym powiedziałem na wstępie – urządzenia zabezpieczenia ruchu kolejowego, wszystko jest sterowane oczywiście mikroprocesorem. Przypomnę, nie wiem, czy państwo pamiętacie, w 2009 r. młody chłopak, chyba uczeń trzeciej klasy technikum, wykoleił w Łodzi tramwaj i zrobił to w bardzo prosty sposób. Nie był to terrorysta, przypuszczam, że nie do końca zdawał sobie sprawę z tego, co zrobił, ale to pokazuje, jak łatwo można zarządzać takimi urządzeniami. Skala pewnych konsekwencji z tym związanych może być duża, a nawet katastrofalna, biorąc pod uwagę pociąg, który porusza się z prędkością 200–250 km/h.

Przewodniczący poseł Bogdan Rzońca (PiS):

Pan prezes, proszę.

P.o. prezesa PKP Informatyka Jakub Prusik:

Jeśli można, bo jak pan prezes będzie kontynuować, to ja musiałbym udzielać odpowiedzi do końca wieczoru. Jeśli można, do wiadomości wszystkich państwa. Po pierwsze, PKP Informatyka monitoruje, niezależnie od tego, czy jest to robione dla klienta, monitoruje infrastrukturę, aplikacje, systemy. W większości są to rozwiązania, które my sami wyprodukowaliśmy, ale nie zawsze. Czasami naszą intencją jest ochrona naszego dobrego imienia, żeby ktoś nie powiedział, że jeśli jest problem informatyczny, to na pewno PKP Informatyka, w związku z tym monitorujemy, żeby powiedzieć – proszę bardzo, sygnalizowaliśmy jakieś zagrożenie, my to zidentyfikowaliśmy pierwsi. To jest jeden temat.

Drugi temat. Bazując, nie tylko, ale to chcę podkreślić, na kontaktach z kolejami samorządowymi, wysłaliśmy nasze propozycje – nie chcę używać słowa oferty, bo to jest wiążące – dotyczące cyberbezpieczeństwa do wszystkich kolei samorządowych. Nie zamykamy się tylko na Grupę PKP. Zresztą w prezentacji i wypowiedziach moich kolegów mowa była o rynku kolejowym. Jeżeli nie zabrzmiało to odpowiednio, to powtórzę, że mówimy przede wszystkim o Grupie, ale jesteśmy nastawieni na rynek kolejowy – zarówno zarządcy infrastruktury, jak i przewoźnicy pasażerscy, towarowi, wszyscy, którzy się na tym rynku znajdują i pod tym mianem podpisują. Jesteśmy otwarci, mamy narzędzia, mamy ludzi.

Następna sprawa. My jesteśmy spółką prawa handlowego, musimy więc świadczyć usługi, żeby z tego mieć wynik dodatni. Mamy w Grupie pewne obostrzenia, nie możemy doliczać marży z sufitu, w związku z tym ona jest niewielka. Staramy się przedstawiać swoje możliwości wszystkim przewoźnikom, również zarządcom infrastruktury, i myślę, że ten proces dość długo się toczy, ale się toczy. Myślę, że w niedługim czasie dojdziemy do wspólnego mianownika, że będziemy mogli sobie podać ręce i wykorzystać pełne możliwości naszego centrum obsługi.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję bardzo. Kontynuujemy dyskusję. Pan przewodniczący Żmijan, proszę bardzo.

Poseł Stanisław Żmijan (PO-KO):

Bardzo dziękuję, panie przewodniczący. Wysoka Komisjo, szanowni państwo, mając w pamięci nasz pobyt, wyjazdowe posiedzenie w siedzibie spółki, a także dzisiejsze informacje, prezentacje i wypowiedzi panów, nie mam wątpliwości, że w tym gronie wiemy, o czym mówimy, i to rzecz jasna, że system budowy w ramach NPC, że udział PKP Informatyka sprowadza się do szeregu funkcji, ale nie najważniejsza jest tutaj możliwość zakupu czy rezerwacji biletu, bo zakłócenie tego procesu przez hakera nie jest groźne, oprócz tego że utrudni życie, wywoła frustrację, nerwy, to nic złego się nie zdarzy. Kluczem jest oczywiście bezpieczeństwo prowadzenia ruchu kolejowego i co do tego nie mamy wątpliwości. Rzecz jasna mam głębokie przekonanie, że zajmujecie się – jako

ludzie kompetentni, co dało się też zauważyć w czasie wizyty, o której mówiłem na wstępie – tym, co trzeba, że nie stoicie w miejscu, wykonujecie pracę, idziecie do przodu. Chwała za to.

Nie sposób nie nawiązać do pierwszej części, czyli wprowadzenia do tematu przez pana ministra. Pan minister bardzo lapidarnie dokonał wprowadzenia, powiedziałbym, że wręcz lakonicznie. Chciałbym, żeby pan minister powiedział więcej o naszej narodowej platformie. Kto odpowiada, zadaję wprost pytanie, kto w resorcie cyfryzacji odpowiada osobiście za tenże narodowy program? Jak on jest realizowany przynajmniej w zasadniczych częściach? Bo tak jak zaznaczyłem, PKP Informatyka będzie tylko małym elementem, proszę mnie dobrze zrozumieć, bo nie chcę powiedzieć niczego złego, ale cyberbezpieczeństwo to najogólniej ujmując, my wszyscy, my – Polska. W związku z tym, panie ministrze, wypadałoby i bardzo oczekujemy, żeby pan powiedział więcej. Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Kto z państwa jeszcze chciałby zabrać głos? Pan przewodniczący Polaczek, proszę bardzo.

Poseł Jerzy Polaczek (PiS):

Dziękuję za udzielenie głosu. Ja może niebezpośrednio nawiązując do dzisiejszej tematyki posiedzenia, ale nawiązując do jednego z aspektów, które na pewno bezpośrednio łączą się z tym, o czym tutaj mówimy, zwracam uwagę – korzystając z obecności przedstawiciel Grupy PKP – na temat, którym w ubiegłym roku zajmowała się Komisja, tzn. kwestię systemu sterowania ruchem interfejsów, bo to jest również potężne wyzwanie do utrzymania zdolności operacyjnej zarządzania tymi kwestiami, choćby przez Polskie Linie Kolejowe. Pomijam tu różne aspekty szczegółowe, bo nie chcę do nich się odwoływać, natomiast jest to jeden z elementów także kosztotwórczych, bo cyberbezpieczeństwo kosztuje, to nie jest tylko kwestia dotacji, ale również kalkulacji kosztów każdego z przewoźników i zarządców infrastruktury, także takiego podmiotu, który swoimi zadaniami wychodzi poza Grupę PKP. Uważam, że powinniśmy w jakimś uzgodnionym terminie, np. nawiązując do tego posiedzenia sprzed roku, które było bardzo specjalistyczne, ale wydaje mi się, że bardzo efektywne, powrócić do dezyderatu pod adresem rządu w tych kwestiach. Sygnalizuję to jako temat na prezydium Komisji, korzystając z tej niewątpliwie ciekawej dyskusji dzisiaj. Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję bardzo. Pan poseł Mrówczyński za chwilkę. Proszę państwa, myślę, że jesteśmy w gronie profesjonalistów i posłowie – mówię za siebie w tym wypadku – może oczekiwaliby podpowiedzi, w czym możemy pomóc w tej materii, bo trzeba patrzeć tu z drugiej strony, nie tylko słuchać, że jest tak i tak, ale być może panowie prezesi, może ministerstwo ma jakieś propozycje dla nas, które byłyby ważne. O tym mówili moi przedmówcy, żebyśmy naświetlili temat z drugiej strony, żeby było lepiej, krótko mówiąc, żeby szybko zrobić to, co musimy zrobić, bo tak naprawdę wszyscy się troszczymy o te coraz większe tłumy ludzi na dworcach kolejowych. Mamy rekordowe wyniki za rok 2018, jak usłyszałem, przewieziono 310 mln osób polską koleją w 2018 r. To są różni operatorzy, różne miejsca, lepsze lub gorsze, to różny tabor, różna obsługa, mniej lub bardziej świadoma, więc gdybyście państwo zredagowali – zwracam się tu do państwa, którzy profesjonalnie zajmują się cyberbezpieczeństwem – to prosimy o pewne sugestie, czym powinniśmy jeszcze się w Sejmie czy na Komisji zająć, żeby ten temat zgłębiać.

Pan poseł Mrówczyński, proszę bardzo.

Poseł Aleksander Mrówczyński (PiS):

Bardzo dziękuję. Panie przewodniczący, Wysoka Komisjo, panowie prezesi, szanowni państwo, nie ulega wątpliwości, że przyszedł taki czas, że trzeba podnieść cały system cyberbezpieczeństwa na wysoki poziom, choćby z racji, o której mówił pan przewodniczący, ilości podróżnych i nie tylko, także daleko idących zagrożeń. Jestem pod wrażeniem prezentacji, bardzo dziękuję, że panowie tak fachowo do tego podchodzicie. To pozwala nam, a przede wszystkim tym, którzy nie mają tak szerokiej wiedzy, przekazać, że dbacie o bezpieczeństwo i czuwacie nad tym. Jest to szalenie ważne.

Przy okazji chciałbym zapytać, bo jeden z panów mówił o wi-fi w pendolino. Nie ukrywam, że obiecywano do końca roku 2018, czas minął, a nadal są problemy. Czy moglibyście podać jakąś datę? Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Czy ktoś jeszcze z państwa zgłasza jakieś uwagi? Nie widzę. Czy pan prezes lub współpracownicy chcą coś powiedzieć lub odpowiedzieć na pytania?

P.o. prezesa PKP Informatyka Jakub Prusik:

Jeśli chodzi o wi-fi, to adres jest trochę inny. Natomiast, jeśli mogę bardziej tytułem uzupełnienia, bo pan prezes i pan przewodniczący mówili o ochronie systemów sterowania ruchem – to jest rzeczywiście docelowo. My nie przez przypadek w jednej z prezentacji umieściliśmy na pierwszym miejscu niski poziom świadomości ludzi. Zawsze na końcu każdego systemu albo na początku stoi człowiek. Jeżeli nie będziemy mieli świadomości zagrożeń urządzeń mobilnych, stacji końcowych, różnych rodzajów ataków… Nam jest dość trudno mówić o obszarze cyberbezpieczeństwa co do konkretnych przypadków, bo one zawsze dotyczą jakiegoś naszego klienta czy partnera. W gronie tak szacownym, jak będziemy bardziej precyzowali, to wszyscy będą wiedzieć, o kim się mówi, nawet jak nie padnie nazwa. Stosunkowo niedawno mieliśmy dość poważny, chociaż krótki atak na jedną ze stron spółek Grupy, który zutylizowaliśmy. Klient się dowiedział post factum, że coś takiego było.

Wracając do ochrony systemu sterowania ruchem, musimy zacząć od ochrony stacji mobilnych, które przy sobie nosimy, stacji końcowych podłączonych przez internet czy inne medium transmisyjne, potem przejść do różnych urządzeń, sterowników, serwerów, a potem wziąć się za systemy sterowania. Musimy to jakoś ustawiać w kolejce, wszystkiego na raz nie zrobimy. Są pewne zaległości technologiczne i organizacyjne, my jesteśmy na to gotowi. Już od dłuższego czasu negocjujemy, nie chcę wywoływać naszych partnerów z PLK, mam nadzieję, że się dogadamy i będziemy mogli powiedzieć, że infrastruktura kolejowa, przynajmniej w części informatycznej, jest zabezpieczana przez nas. To tyle z mojej strony.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję bardzo. Pan minister, proszę bardzo.

Sekretarz stanu w MC Adam Andruszkiewicz:

Szanowna Komisjo, odpowiadając na pytanie, kto w Ministerstwie Cyfryzacji zajmuje się stricte tworzeniem i koordynowaniem Narodowej Platformy Cyberbezpieczeństwa, to jest to sekretarz stanu, pan minister Karol Okoński, który jest przy okazji pełnomocnikiem rządu do spraw cyberbezpieczeństwa. Jest to wybitny fachowiec i to on bezpośrednio tę kwestię nadzoruje, wdraża i myślę, że w każdej chwili jest w stanie odpowiedzieć na państwa pytania. Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Proszę bardzo, panie prezesie.

Członek zarządu PKP Informatyka Radosław Zawierucha:

Dziękuję. Chciałbym się odnieść do wypowiedzi szanownego pana posła z prezydium. Oczywiście mamy świadomość pewnej gradacji zagrożeń i sterowanie ruchem kolejowym jest na samej górze tej piramidy hierarchii. Natomiast, nie chcąc przedłużać wypowiedzi, równie dużą wagę trzeba przykładać do ruchu pasażerskiego, bo to nie jest tylko zabezpieczenie procesu zakupu biletu czy rezerwacji lub trafienie klienta do właściwego pociągu, ale – podam na przykładzie – proszę sobie wyobrazić, że poprzez system informacji pasażerskiej wpływa się istotnie na kierowanie potoków ludzkich. Na dużych dworcach to jest niebagatelna sprawa. Wyobrażam sobie bez problemu taką sytuację, że poprzez ingerencję w system kieruje się wszystkich podróżnych na jeden peron, a na tym peronie… Proszę sobie już dalej dopowiedzieć, co się może wydarzyć. Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Proszę bardzo.

Poseł Stanisław Żmijan (PO-KO):

Oczywiście, że tutaj się nie różnimy w ocenie – mimo wszystko bezpieczeństwo szeroko rozumiane, prowadzenie ruchu na naszej sieci jest po prostu na najwyższej półce i to jest zrozumiałe. Podwyższenie standardu i ułatwianie sobie, czynienie podróży przyjemnej to jest jasne i oczywiste, ale przede wszystkim zabezpieczenie prowadzenia ruchu, a więc to, o czym jeden z panów mówił, chyba pan prezes Góra, że nastolatek – świadomie czy nieświadomie – wykoleił tramwaj. O tym mówimy i oczywiście nie różnimy się w postrzeganiu sprawy. Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję bardzo. Czy są jeszcze jakieś pytania, uwagi? Czy możemy uznać zatem, że wyczerpaliśmy temat naszego spotkania? Oczywiście z tymi zadanymi pytaniami pozostawiamy specjalistów. Gdyby do prezydium chcieli państwo skierować jakieś propozycje w tej materii co do potrzeby głębszej analizy czy rozwiązań prawnych, bo od tego jesteśmy jak najbardziej, jeśli możemy pomóc państwu w czymś, to służymy pomocą, bo chcemy, żeby wszędzie było bezpiecznie. To pierwsza potrzeba człowieka. Bardzo proszę, panie prezesie.

P.o. prezesa PKP Informatyka Jakub Prusik:

Przepraszam, jeśli można. Czuję się trochę wywołany do tablicy. Mamy jakiś problem organizacyjno-prawny, nie tylko w obszarze cyberbezpieczeństwa. Mamy spółki z Grupy, jesteśmy spółką prawa handlowego, oni też, w związku z tym nie mogą z wolnej ręki nam pewnych spraw zlecić. Każda ze spółek ma próg zamówień, według swojego regulaminu, reszta idzie w PZP. Obszar cyberbezpieczeństwa jest obszarem bardzo delikatnym, dotykamy danych, które muszą być nie tylko chronione, ale też archiwizowane. Nie można ich powierzyć w prywatne ręce, nawet gdyby to były najszlachetniejsze prywatne ręce. Przepraszam za duży poziom ogólności.

Jeżeli pan przewodniczący wyraził wolę pomocy, to gorąco prosimy o pomoc. My na dziś, po półtora roku różnych negocjacji, nie wiemy jak zrobić, żeby np. PLK mogły z wolnej ręki nam zlecić coś, co my jesteśmy w stanie wykonać. Przepraszam, że mówię bez ogródek. Dziękuję bardzo.

Poseł Stanisław Żmijan (PO-KO):

Przepraszam, Wysoka Komisjo, pan prezes sprowokował mnie do wypowiedzi. Ja się z panem całkowicie zgadzam, z tezą, którą pan wyraził, ale wobec tego, jakie mamy doświadczenia z ostatnich tygodni, miesięcy, powiem krótko – odsyłam pana prezesa na konsultacje do ministra Błaszczaka, on naprawdę wie, jak to się robi, z wolnej ręki zakupy dla armii w ostatnich miesiącach. Nie oczekuję komentarza. Dziękuję.

Przewodniczący poseł Bogdan Rzońca (PiS):

Dziękuję bardzo. W takim razie pozwolę sobie podziękować państwu za obecność. Zamknęliśmy pewien rozdział i otworzyliśmy następny do ciekawej debaty. Proszę więc o sugestie, a na dzisiaj – dziękując państwu za obecność i wypowiedzi – zamykam posiedzenie Komisji.